th

13th ICCRTS: C2 for Complex Endeavors

Assessment of Electromagnetic and Passive Diffuse Infrared Sensors in Detection of IED-Related Behavior

Topic 2: Networks and Networking (also Topics 7 and 8)

Joshua Sundram (STUDENT), Phua Poh Sim (STUDENT),

Neil C. Rowe, and Gurminder Singh

Point of Contact: Neil Rowe (ncrowe@nps.edu)

Naval Postgraduate School

Code CS/Rp, 1411 Cunningham Road, Monterey CA 93943

(831) 656-2462

jsundram@nps.edu, pphua@nps.edu, ncrowe@nps.edu, gsingh@nps.edu

Abstract

Persistent wireless sensor networks can be a cost-effective way to monitor public areas for suspicious behavior and reduce the need for military patrols. We examine here their applicability to the difficult problem of detecting emplacement of improvised explosive devices (IEDs). We first discuss the threat and how wireless sensor networks could help fight it; flexible and adaptable management of the sensor network is essential. We then report some experiments with magnetic and infrared sensors from Crossbow Technologies. We built a network of these sensors and ran human subjects through it engaged in various activities, some involving carrying of ferromagnetic materials. Results indicated that a variety of suspicious activities could be detected, though not all mock IEDs triggered detection, and triangulation was difficult due to the tendency of the signal to quickly saturate. Our network design is such that data can be easily aggregated in larger networks for broad-area automated monitoring of settings such as airports and busy urban areas.

Keywords: sensors, magnetic, improvised explosive devices, detection, testing, networks

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assessment of Electromagnetic and Passive Diffuse Infrared Sensors in Detection of IED-Related Behavior	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Code CS/Rp,1411 Cunningham Road,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT

Persistent wireless sensor networks can be a cost-effective way to monitor public areas for suspicious behavior and reduce the need for military patrols. We examine here their applicability to the difficult problem of detecting emplacement of improvised explosive devices (IEDs). We first discuss the threat and how wireless sensor networks could help fight it; flexible and adaptable management of the sensor network is essential. We then report some experiments with magnetic and infrared sensors from Crossbow Technologies. We built a network of these sensors and ran human subjects through it engaged in various activities, some involving carrying of ferromagnetic materials. Results indicated that a variety of suspicious activities could be detected, though not all mock IEDs triggered detection, and triangulation was difficult due to the tendency of the signal to quickly saturate. Our network design is such that data can be easily aggregated in larger networks for broad-area automated monitoring of settings such as airports and busy urban areas.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**39**	

th

I. Introduction

Improvised-explosive devices (IEDs) are "homemade" bombs containing explosives (military or civilian) attached to a detonator and an initiating mechanism (U.S. Army, 2005). "The IED continues to be the single largest threat that coalition forces face in Iraq; there were 11784 known IED-related incidents in 2004" (CRS, 2005). To 2006, IEDs in Iraq claimed more than 1500 lives and injured many thousands (Grant, 2006). Usually considered a form of asymmetric offense, IED incidents can result in significant fatalities and collateral damage and are becoming the weapons of choice for the terrorist groups and insurgents. IEDs can be devastating weapons due to their ease of targeting state assets such as soldiers, government officials, transportation infrastructure, and aid vehicles. IEDs are inexpensive but expensive to combat. It is reported that about $6.1 billion has been spent on U.S. efforts to defeat IEDs. But current countermeasures have only been partially effective despite these expenditures.

This work explored the use of persistent sensor networks to detect emplacement of IEDs. Emplacement is an inherently a suspiciously appearing action, and perhaps the best time to foil an IED. Video surveillance can detect emplacement, but it requires many cameras and personnel time to monitor them. Nonimaging sensors can be cheaper per unit area of coverage yet still detect loitering and other suspicious actions. However, many technical problems need to be solved to use sensors effectively for this task. This work is a first step.

II. Background

A. Characteristics of IEDs

IEDs are used almost exclusively by rogue entities with the intent of achieving an asymmetric tactical advantage over the adversary (U.S. Army Training and Doctrine Command, 2007). The DOD-NATO definition is "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract; it may incorporate military stores, but is normally devised from nonmilitary components." They are bombs much like mines and implemented in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals. They are designed to destroy or incapacitate personnel or vehicles (U.S. Army, 1992). IEDs are usually command-detonated and are emplaced with specific targets and windows of opportunity in mind (as offensive in nature). Mines, on the other hand, are often used in defensive postures such as border defense, denial of access to main supply routes, etc. and are triggered by pressure or a tripwire (non-command detonation). IEDs are typically composed of an explosive charge, a detonator, and an initiating system.

IEDs are usually packaged with surrounding materials (PIEDs). They may be hastily camouflaged with dirt, rocks, trash or items that are commonly found on the roads, and

th

can range from a small beverage can to something larger such as an artillery shell. They may also be put in vehicles (VIEDs) or used in suicide bombings. Most are initiated by an electrical wire since this allows for precise timing of the explosion and immunity to electronic jamming. Organizations that deploy IEDs are small and typically consist of six to eight personnel, including bombmakers, emplacers, and triggermen who actually detonate the IED at an opportune moment (Defense News, 2005). While it is useful to attack the entire IED delivery structure, it is often easiest to disrupt the IEDs by stopping emplacement because that is when the IED is most detectable.

IEDs can be emplaced almost anywhere there is sufficient space for concealment and there are possible vantage points for activation when targets come into view. However, IEDs are most likely to be emplaced along main routes such as supply routes that are heavily used by an adversary. Common IED locations are past successful emplacements, trees, bridges, lampposts, checkpoints and other places that vehicles frequently stop. Statistics on media-reported IED occurrences in Iraq and Afghanistan from June 2006 to June 2007 show that there were 44 in city squares, 168 in or adjacent to roads, and 163 in indoor spaces. This suggests we should focus on studying the last two.

B. IED Detection

Most research on foiling IEDs has focused on detecting them once emplaced, but this is difficult. Some indicators of emplaced IEDs are similar to those of conventional booby traps, such as disturbed soil and sand, isolated boxes and containers along common roads, or exposed trip wires, strings or cables left behind by the perpetrators intentionally or accidentally. Other indicators include:

- People on overpasses
- Signals from vehicles or bystanders
- Unattended containers
- Markers by the roadside serving as possible aiming references
- Disturbances of the ground surface
- Improvised methods of marking such as piles of stones or marks on walls or trees
- Metallic objects such as drink cans and cylinders
- Videotaping of seemingly ordinary activities or military activities
- Unusual behavioral patterns such as the absence of women and children, or a noticeably reduced number of vehicles or people in a normally busy period

Such indicators can be sought by a variety of automated methods using aerial surveillance, handheld devices, unmanned ground vehicles, or unmanned aerial vehicles (Hannum, 2007). Detection can be active or passive. Passive detection methods include various chemical means for the remote detection of explosive material such as chemoluminescence, high-speed gas chromatography, and specialized electronic sensors (Collins et al, 2006). Magnetic sensors are helpful since most IEDs contain steel (Hoke et al, 2005). As for active detection, (XyTrans, 2006) offers a product using MMW radiometers to detect slightly disturbed soil and vegetation that suggests buried IEDs. Another approach is to bombard material with radiation or particles to look for signatures

th

of nitrogen compounds in explosives such as TNT and C4. Work on chemical nanosensors offers the promise of high sensitivity and fast detection.

Most of these methods have high false-alarm rates because there are many types of materials in the world and it is difficult to tune detection to recognize only one kind. While legislative controls such as denying access to precursor chemicals used to manufacture explosives may also disrupt IED deployment, it would seem better to focus on detection of IED emplacement because the emplacer must necessarily exhibit some suspicious objects and execute some suspicious activities such as excavation and leaving an object behind. That will be our focus here.

C. Wireless Sensor Networks

A wireless sensor network is a collection of sensor nodes that are organized into a cooperative network; they are "ad-hoc systems" containing sensors connected by wireless links (Akyildiz et al, 2002). Wireless sensor networks have numerous applications, ranging from habitat monitoring to environmental control, and in the military realms of intelligence, surveillance and reconnaissance (ISR). Sensor networks have the advantages over other surveillance technology of a widely distributed presence, minimal intrusiveness, and minimal need for human interaction (Haenggi, 2005). Detection of IEDs could benefit from them because sensor networks are increasingly used to cooperatively detect and identify targets of interest. Sensor nodes picking up suspicious activities could forward the data via repeaters to relay stations and notify backend operators and analysts, whom could activate services such as the rescue teams, fire brigades, and law enforcement agencies.

The sensor system that we explored in our experiments was the Crossbow MSP410, which comprises of sensor nodes (termed “motes”) in 8-sensor groups along with a “base station” (Figure 1). It is made by Crossbow Technology (www.crossbow.com). Each mote of type MSP410A contains a magnetic and a passive infrared sensor. The passive infrared sensors provided coverage of 30 degrees vertical and 90 degrees horizontally, detected wavelengths from 5 to 14 microns, and were claimed to detect humans within 30-40 feet and cars within 50-60 feet. The magnetic sensors were two-axis magnetic-field "disorder" detectors that note changes to the magnetic field with a field range of plus or minus 6 gauss, sensitivity 1 mV/V/gauss, and a resolution of 120 microgauss for a 50 hertz bandwidth. Earlier experiments on tracking people with this equipment were promising (Salatas, 2005).

th

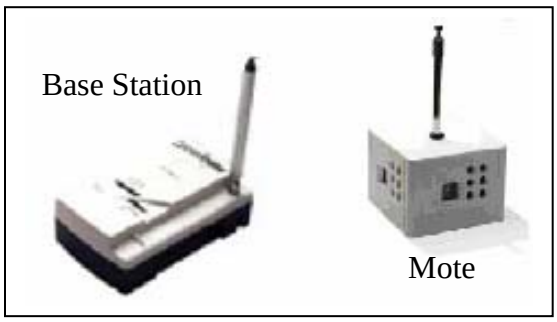


Figure 1. Crossbow MSP410 Base Station and Mote.

Wireless sensor networks appear promising for detecting IED emplacement because they can provide uniform coverage of a wide area. Surveillance by camera provides only a limited number of perspectives and can suffer from occlusion problems. Furthermore, sensors of a variety of different modalities can provide robust and more accurate detection of IEDs (Tran et al, 2007) than can imaging alone. Diffuse passive infrared and magnetic sensors appear good at finding suspicious behavior of both people and vehicles (Caruso and Lucky, 2007), they can be cheaper than cameras, and the necessary data processing can be simpler than that for images. Magnetic sensors are particularly good at vehicle detection (Rouse et al, 1995) and have been used for detection of unexploded ordnance (Wiegert & Oeschger, 2006). Diffuse passive infrared detectors are a mature technology with many applications, and just a few infrared sensors can accomplish complex monitoring tasks (Kaushik, Lovell, & Celler, 2007). There are additional problems with processing to track and detect suspicious behavior which we have addressed in previous work (Rowe, 2005).

D. Command and Control for IED Detection

Since IED detection requires a wide range of techniques, coordination of efforts is essential by a carefully designed command-and-control structure. Priorities and deployment parameters need to be assigned to the techniques. For instance, one must decide how valuable is it to use chemical sensors to detect explosives versus putting detectors on booms in front of vehicles versus doing video surveillance. This analysis then determines the allocation and deployment of personnel and equipment.

Sensor networks can be considered as an extension of a military command-and-control hierarchy where devices are patrolling rather than soldiers. With a varied set of sensors, instructions analogous to orders are given as to what information to collect. With software control, instructions can be changed quickly as the situation in the sensor field develops. IED detection methods particularly need to be reviewed periodically as enemies adapt. Adaptation is an important phenomenon today in Iraq; for instance, IED emplacers quickly shifted in the course of a year from radio-wave triggering to command-wire triggering (Atkinson, 2007). This means the clues to look for as to IED emplacement change too, since we can now look for evidence of wires being laid to the device. It is thus helpful for IED detection to focus on general-purpose knowledge of the

th

observed behavior such as tracks and accelerations rather than trying to identify specific signatures of an IED emplacer. That has been our strategy here.

III. Experimental Methodology

A. Test Cases

We give an overview of our experiments here; more details are in (Sundram & Sim, 2007). Test Case A used public areas, but Test Cases B, C and D used locations at our school so that we could control the test signatures more closely using human and vehicular actors. Figure 2 shows our simulated mall and roadside designs including such representative objects as lampposts, escalators, and trash bins. "IR" means "infrared" and "M" means "magnetic".

Thresholds were established for normal infrared and magnetic signature readings to determine when foreign entities with abnormal signatures entered the test environments. The independent variables in these tests were N, the number of sensors; X, the amount of ferrous material (measured in the number of nails); H, the height of a sensor node above the ground; d, the distance from the Crossbow sensors; and t, the thickness of a trash bin.

Test Case A was conducted at a quadrangle outside a mall (Test Environment A) and along a one-way street (Test Environment B) during both peak (1200-1400) and off-peak (1600-1800) periods. The sensor motes were located at ground level, and were interspersed at roughly equal spacings acknowledging restrictions due to the terrain.

Test Case B examined the amount of ferrous content and distance d which were required to trigger the Crossbow magnetic sensors by an actor carrying nails into the test environment. It also attempted to determine a feasible topology of sensors for effective detection.

Test Case C examined to what extent electrical hardware simulating IED initiators could be detected by magnetic sensors. The main ferrous component of IEDs that are commonly emplaced in postal or trash receptacles are usually electrical circuit boards.

Test Case D simulated the deposit of an IED in a trash receptacle. This tested the robustness of the sensors in detecting and reporting foreign magnetic signatures as well as the effects of the thickness of the trash receptacle and the waste items. Trash receptacles are tempting for IEDs since they are common to all types of environments, are publicly accessible, and provide shrapnel. The U.S. Department of Homeland Security "Approved Product List for Homeland Security" recommends "blast resistant trash receptacles" (U.S. DHS, 2002).

th

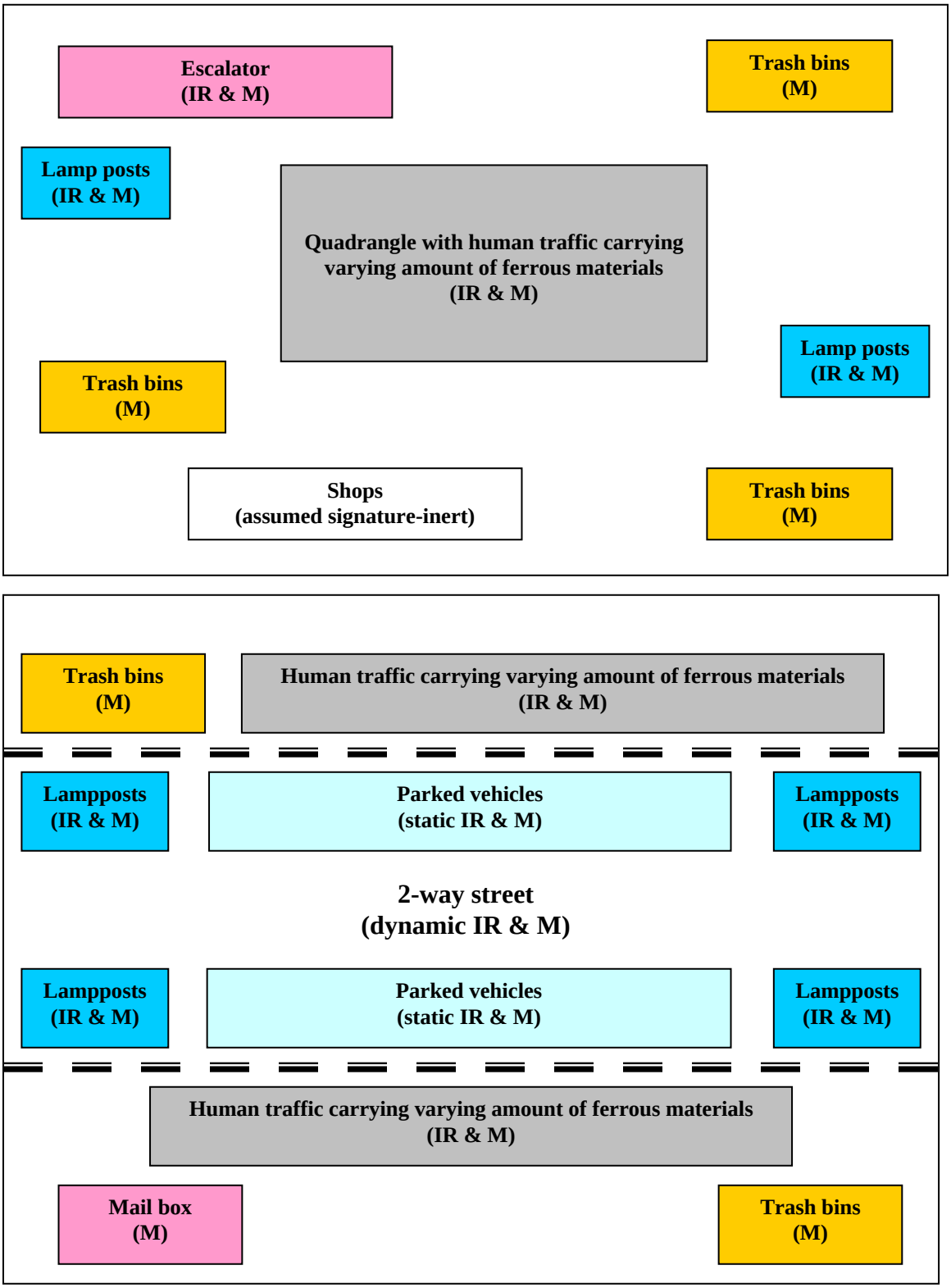


Figure 2. Layout of a simulated roadside/street test environment.

th

For Test Case D, an actor carried circuitry into the simulated test environment and approached a trash receptacle along a fixed path, then dropped circuitry into it (Figure 3). The circuitry was from a remote-controlled toy, to simulate wireless-controlled IEDs. Two motes were used, one in the trash bin and one beside it. The bin was filled with common household trash (rubber, textiles, leather, plastics, metals, glass, paper and food scraps). Two subexperiments investigated the effects of the receptacles' thickness and the effects of the emplacement force on the sensitivity of the magnetic sensors. Thicknesses of typical trash receptacles range from 0.2 cm to no more than 1 cm, so experiments were conducted for t = 0.2 cm, 0.5 cm and 1 cm, and H = 0 cm, 45 cm and 90 cm. The height of the trash was assumed to be 1/3 the height of the trash bin. Common household plastic was wrapped around the main housing of the trash receptacle to increase t.

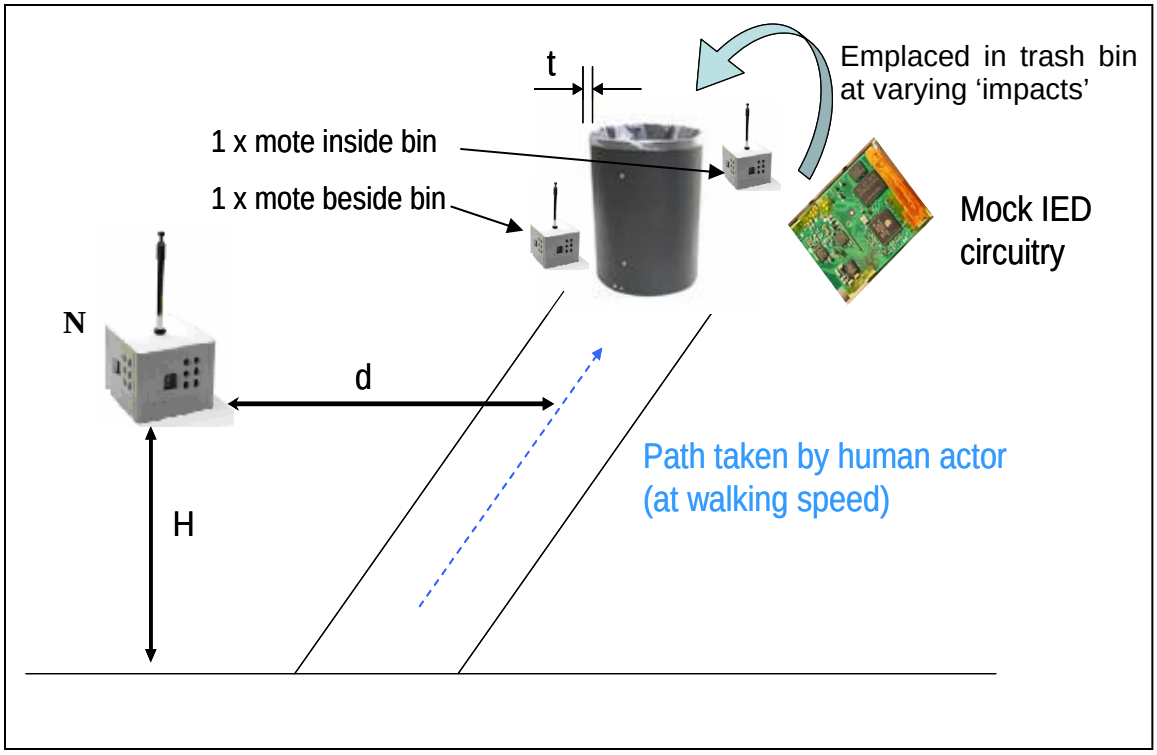


Figure 3: Setup of Test Case D.

B. Detection Methods

The process of detecting events using the Crossbow sensors was:

- Collection of raw data from Crossbow motes on foreign infrared and magnetic signatures;
- Identifying and extracting the relevant packets from the data;
- Comparing readings with thresholds through a database server;

th

- Issuing a signal or alert to the user platform upon positive identification.

Crossbow's software for accessing and managing motes is MoteView, SerialForwarder, and TinyOS (the operating system). MoteView is a user controller for the sensor system which comes with the development kit. It works on a three-layer architecture using a mote layer, a server layer, and a client layer; MoteView operates in the client layer. Depending on the program which is used in the Crossbow motes (usually compiled in TinyOS environment), the data is captured in accordance to the programmed tasks and is stored or logged in the databases in the server layer. From here, the user can retrieve selected data on the MoteView screen. There are options to view the data logged in the server layer as raw data, measurement data (raw data converted to appropriate units of measure), charts, or in a spectrum view.

Surge-View is a set of software tools including the Surge Graphical User Interface, the Stats, and the HistoryViewer programs. SerialForwarder reads packet data from a computer's serial port and forwards it over a server port connection, so that other programs can communicate with the sensor network via a sensor network gateway. SerialForwarder listens for network client connections on a given TCP port, and forwards TinyOS messages from the serial port to the network client connection and vice versa. Many TinyOS applications run with the support of the SerialForwarder program upon startup such as Listen.class.

TinyOS is an open-source operating system that runs embedded in sensor nodes and is used in many wireless sensor networks. It contains built-in interfaces, software components, and configurations that programmers can use to build their applications. One component, the Listen class, reads sensor data upon a trigger of events from the mote that senses, and this component is vital for tracking of objects. As the motes would report on all foreign signatures within its sensitivity range, we had to modify Listen.class so only those signatures exceeding a particular threshold would be reported. Thereafter the motes would resume idle mode. Typically the motes are able to distinguish and report two signatures occurring separately in the order of milliseconds as independent events as indicated by the timestamps (with an unique sample number attached to each event), i.e. 12:30:10 for sample #200 and 12:30:10 for sample #201.

IV. Experimental Results

A. TEST CASE A

The motes could effectively sense the presence of human agents in a real-world environment with infrared sensors. Figure 4 shows example readings. There were frequent triggers throughout the 30-minute period, and an observable difference between the peak and off-peak period. Magnetic triggers, on the other hand, were infrequent and sporadic as indicated by the spikes. This suggests that few agents carry ferrous materials (maybe just laptops) or that sensor motes are not very sensitive to magnetic signals. It

th

also means that establishing a magnetic threshold using the mean value would not be accurate. Some inefficient coverage of the test environment resulted from spatial constraints in the quadrangle, as well as the limited number of motes (8) that we had for the experiment.

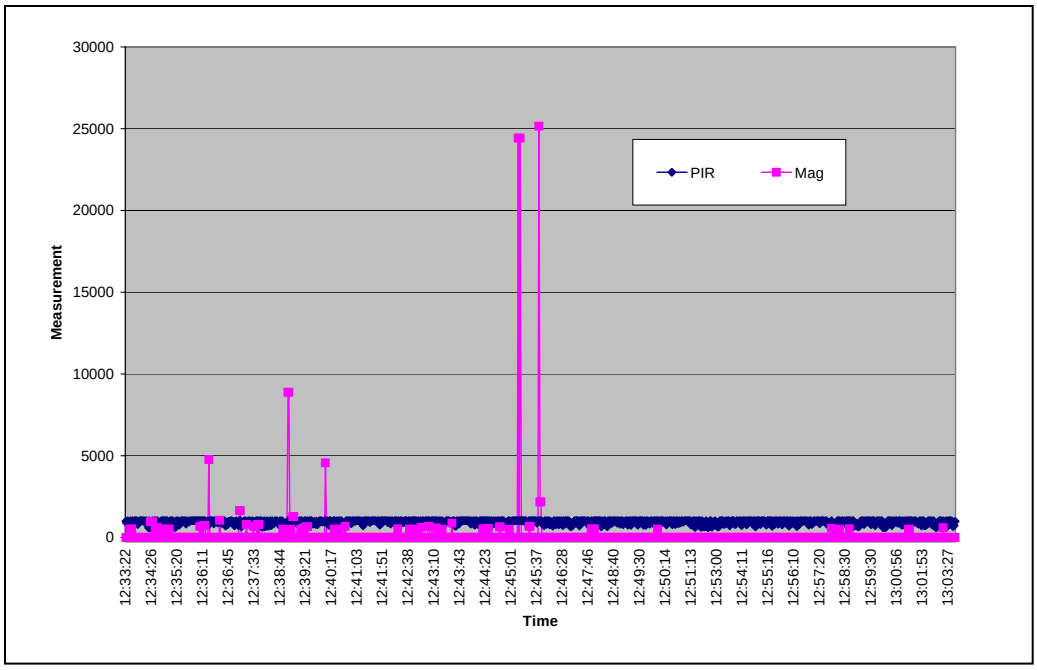


Figure 4: Infrared and magnetic readings during a peak period in test environment A of Test Case A.

In test environment B for Test Case A, with vehicular movements unlike environment A, there were frequent magnetic triggers with corresponding passive infrared detections (the heat from engines). However, there were positive magnetic triggers without any change in passive infrared (for the base level of 1023 units) as highlighted in Figure 5, which could reflect a cold vehicle engine just turned on or fluctuations in ambient temperatures. (Electromagnetic interference should not be a problem with Crossbow sensors as its magnetometers have a bandwidth of 400 Hz or less, so even strong radio-frequency sources like cell phones and base stations should not affect magnetic readings.) Another possible cause could be the limited field of view of the motes so that a single vehicle would be perceived as separate objects, a heated engine and a cold body. The large average magnetic reading of 950 units suggests that magnetic sensors alone in such an environment may not detect PIEDs which contain a low ferrous content.

th

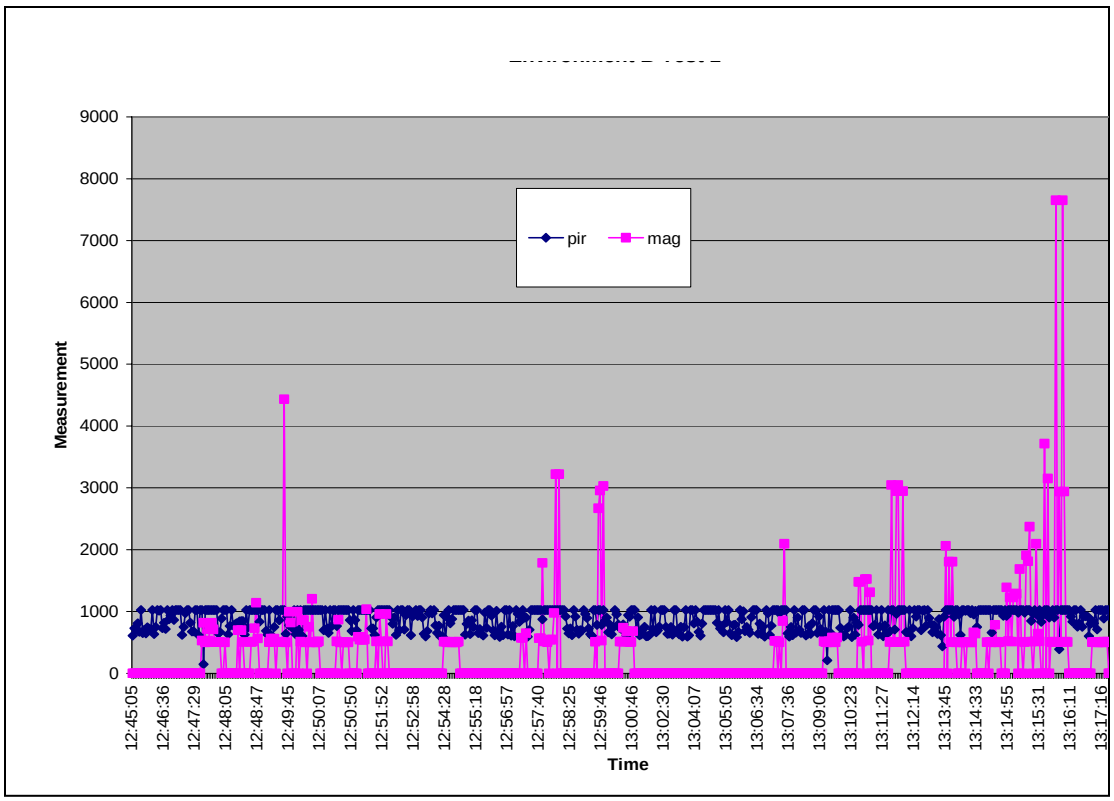


Figure 5: Infrared and magnetic readings during peak period in test environment B of Test Case A.

Table 1 shows the inferred thresholds found for Test Case A. In both cases, the peak period was 1200-1400 hours and the off-peak period was 1600-1800 hours.

B. TEST CASE B

Unsurprisingly, Test Case B showed higher magnetic readings for nails closer to the motes than further away. There were also fewer false positives for H = 45 cm and 80 cm than for H = 0 cm or ground level for sensor height. This could be attributed to the sensors' two-axis magnetometer circuit boards which are aligned horizontally when placed flat on a surface. The low false negative rate for H = 45 cm and 80 cm is encouraging as these are the heights that agents are expected to carry IEDs.

th

Test Environment A		Test Environment B	
Peak period			
Magnetic	**Infrared***	**Magnetic**	**Infrared**
1375	695 (-)	22147	420 (-)
Off-peak period			
520	987 (-)	21460	413 (-)

***Original infrared value for Crossbow sensor is at 1023units. The detection of presence of IR is represented by a decrease in the original infrared value hence the (-).

Table 1. Tabulation of thresholds for Test Case A, test environments A and B.

Crossbow recommends deployment configurations called "dense grids" (uniformly placement in an area) and perimeter grids (uniform placement on the perimeter of an area). Our experiments were conducted using the dense-grid deployment with the motes positioned at intervals of 5 feet (the recommended spatial interval is 40 ft). Two deployment directions of the motes were tried; the deployment with sensors at 45 degrees to the path direction was more sensitive (with magnetic readings exceeding 1000 units) than that with sensors orthogonal to the path. This could be due to the magnetic sensor axis (located along the sides of each mote) having a greater area of exposure to signals from the passageway.

20 runs were done of the experiment for each of heights of 0, 45, and 80 cm and d=10 and 50 cm. The number of nails was 5, 10, and 20, and the actor used a normal walking pace. Table 2 shows the averages of the readings.

th

***X* / nails**	**Magnetic readings at H / cm**					
	0		**45**		**80**	
	Distance from mote, d / cm					
	10	**50**	**10**	**50**	**10**	**50**
5	207	144	559	560	488	492
10	215	150	667	596	654	512
20	219	184	882	598	886	534

Table 2. Tabulation of magnetic readings for test case B.

C. TEST CASE C

Test Case C was like Test Case B except for the replacement of nails with circuitry. Similar average magnetic readings were observed for circuitry although they were dissimilar in forms and sizes (Table 3). This suggests that threshold-categorization of IED circuitry may not be possible using magnetic sensors alone as many other objects many trigger readings within the threshold range.

H / cm **d / cm**	**Magnetic Readings**		
	0	**45**	**80**
10	294	589	680
50	221	578	619

Table 3. Tabulation of magnetic readings for test case C.

D. TEST CASE D

Figure 5 shows another view of the experimental setup for Test Case D. The force of depositing trash may be a useful indicator of IED emplacement and the Crossbow magnetic sensors can detect it. Two cases were investigated, gradual versus sudden emplacement for t = 0.2 cm and H = 90 cm. "Gradual" was defined as a gradual movement of a mock IED into the mouth of the trash receptacle and placing it just above the trash whereas "sudden" was defined as dropping the mock IED from the mouth of the trash receptacle. Average readings were 539 for gradual emplacement and 819 for sudden emplacement (Figure 7). Some of the sensors could detect the human actor carrying the circuitry (with the showing of an alert in our implementation) as he approached the trash bin, but there were occasional false negatives by some motes when the actor was out-of-range.

The two motes at the bin were largely successful in detecting the mock IED as it was dropped in the bin. The mote inside the bin had a 100% positive detection. The mote outside the bin registered lower magnetic readings and displayed similar trends as Test Case C, i.e. a number of false negatives for H = 0 cm, and 100% positive detection for H = 45 cm and 90 cm. The magnetic readings had several spike outliers possibly attributable to the disturbance of the mote as the mock IED was dropped, as movement of the mote also causes a change in magnetic flux. The results for various bin thicknesses confirm an inverse relationship between a bin's thickness and the strength of magnetic readings (Table 4). Consequently, the mote outside the bin for t = 1 cm had a higher frequency of false negatives.

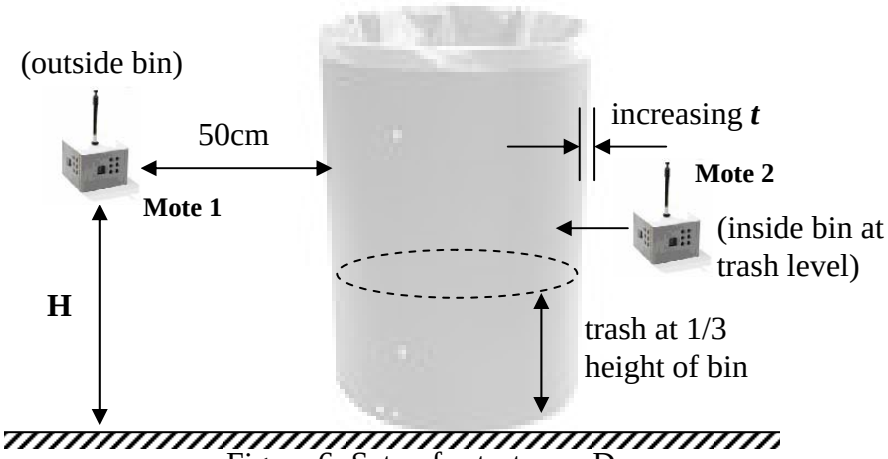


Figure 6: Setup for test case D.

th

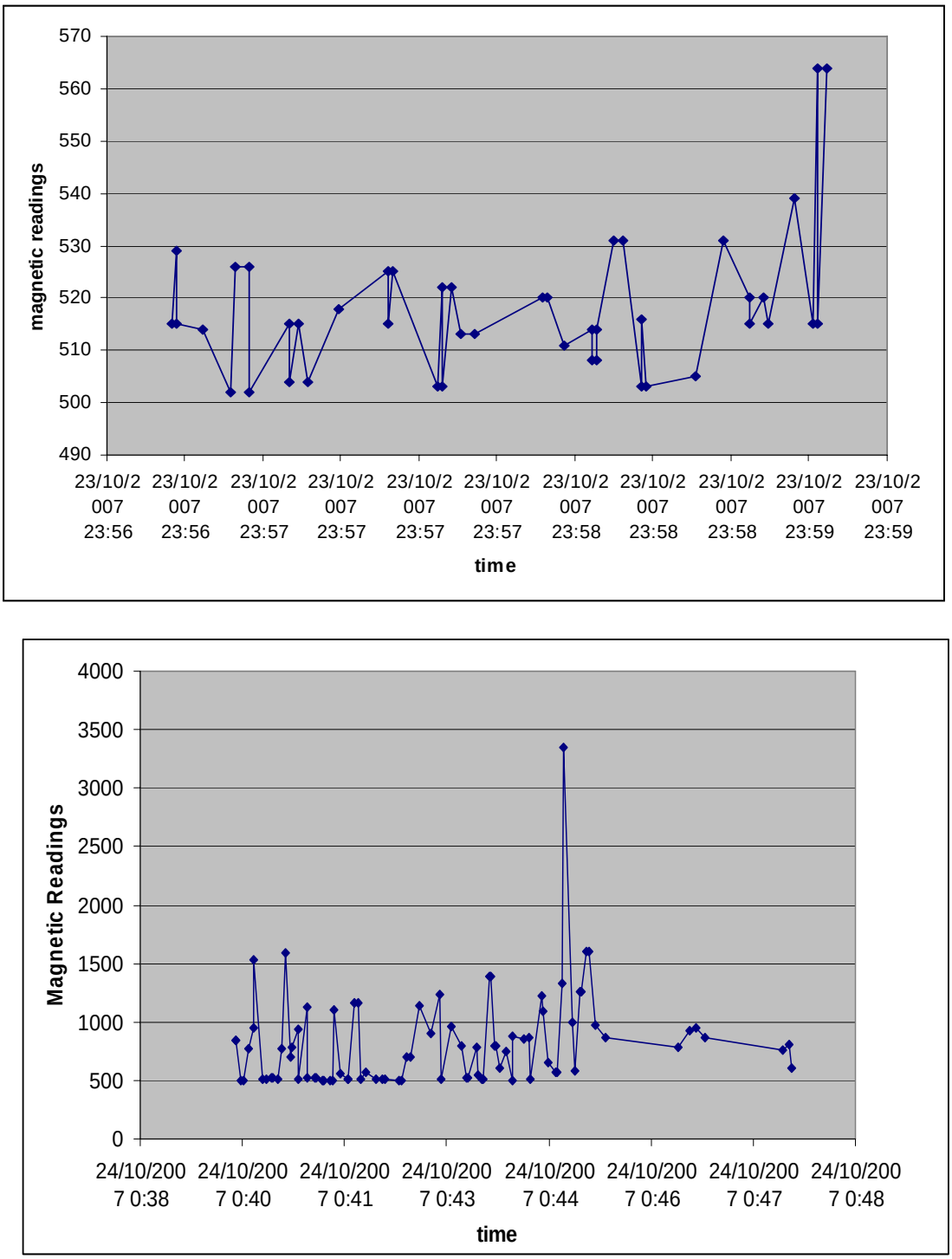


Figure 7: Magnetic readings for gradual (top) and sudden (bottom) emplacement.

th

H / cm t / cm	Mote 1			Mote 2		
	0	**45**	**90**	**0**	**45**	**90**
0.2	0	483	497	509	516	539
0.5	0	285	455	-	-	-
1	0	268	421	-	-	-

Table 4. Tabulation of magnetic readings for test case D (variation with bin thickness t).

V. Conclusions

Detection of IED emplacement is a very difficult problem, and this work is just a start. However, Crossbow sensors demonstrated useful capabilities for it. Magnetic sensors could detect suspicious ferromagnetic materials near and in the trash receptacle, and infrared sensors could distinguish the presence of small numbers of people. Key findings were:

- Crossbow sensors have trouble characterizing small objects. Even for larger objects, other sensing modalities will help describe the granularity of materials so that there is a distinct contrast among their characteristics.
- The thresholds established in our experiments were averages of the readings, but such a computation is crude. Thresholds need to take into account time of day and week, and what activities are occurring in the sensor field.
- Crossbow's diffuse infrared sensors are good at detecting human traffic but this is not useful for IED detection by itself. Not all close objects were detected because the sensing beams used a narrow angle more appropriate for motion detectors.
- The infrared sensors were susceptible to air disturbances and temperature variations, and the magnetic sensors triggered even in the absence of ferrous materials. However when placed in more restricted deployments such as in receptacles, magnetic sensors may be more helpful.
- Our experiments used a limited number of sensor motes. Using more motes and correlating their data to find consistent phenomena should help reduce false positives.
- The sensor topology we used appears to be a good deployment template for threat scenarios where there are limited ingresses and egresses.
- Power consumption is an important limitation in any outdoor deployment of wireless sensor networks. Our experiments required high levels of power consumption because the motes reported data frequently. Each mote uses two 1.5-volt alkaline AA batteries, and the mote's lifespan is estimated at 250 hours

th

and 12000 hours for constant active mode and sleep mode respectively (based on the estimated power consumption rates from (Davis & Miller, 2007)). Though there are algorithms to allow sensors to adapt when one or more motes are not functioning, the issue of power supply must be carefully addressed (i.e. simulation of power consumption) prior to deployment.

Our future research will explore several ideas:

- Acoustic sensors provide a different kind of signal strength that is reasonably reliable for triangulation. Furthermore, the pattern of the signal (footsteps, engines, dragging sounds, etc.) gives good clues as to its identity.
- Chemical sensors are an important part of an anti-terrorism arsenal. They can detect chemicals of explosive materials, burning materials, poisons, etc. While rarely expected to be triggered, they can provide a valuable independent dimension of data.
- While cameras can be expensive and suffer from occlusion problems, imagery (either visual or infrared) could provide useful data not easily obtained by other sensors. It also greatly helps the providing of "ground truth" for experiments.
- Triangulation methods need to be developed for tracking of objects moving in the sensor field, as locating the threat source is just as vital as its detection, and a positive localization can minimize unnecessary disruptions like cordoning and crowd dispersal. Triangulation is a challenge since most of the sensors we are considering provide only a signal strength and not a direction, but sufficient quantities of sensors can compensate for their limitations.
- Adaptability is essential in anti-terrorism sensor networks. We need to develop software techniques to aggregate sequences of sensor events into larger units so that we can detect subtler patterns where no one event is by itself suspicious. For instance, we need to detect a sequence of possibly digging a hole, possibly emplacing a device, and possibly running a wire to it. Even if we are uncertain about the events, certainty about suspiciousness of the whole sequence may be higher.

References

Akyildiz, I., W. Su, Y. Sankarasubramaniam, & E. Cayirci. 2002, August. A survey on sensor networks. *IEEE Communications Magazine*, Vol. 40, No. 8, 102-114.

Atkinson, R. 2007. Left of boom. *Washington Post*, September 30-October 3.

Caruso, M., & S. Lucky. 2007. Vehicle detection and compass applications using magnetic sensors, Honeywell Inc. Available from www.magneticsensors.com/datasheets/am.pdf, last accessed 15 Sep 2007.

Collins, G., A. Haes, Q. Lu, & B. Giordano. 2006, October. Lab on a chip sensor platform for explosives and CBW toxin detection. *Proc. Intl. Workshop on Measurement Systems for Homeland Security, Contraband Detection*, and Personal Safety, 2-4.

th

CRS. 2006 (September). *Report for Congress – Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures.* Available from research.fit.edu/fip/documents/SecNews1.pdf, last accessed 9 Aug 2007.
Davis, H., & R. Miller, Power management for Mica2 motes. Department of Computer Science, North Carolina State University. Available from www.cs.etsu.edu/sasplas/papers/davis-miller%20paper.doc, last accessed 30 Oct 2007.
Defense News. 2005 (August). The IED marketplace in Iraq. Available from globalguerrillas.typepad.com/globalguerrillas/2005/08/the_ied_marketp.html, last accessed 15 Oct 2007
Grant, G. 2005 (March). US begins to counter IED threat. *Jane's Defense Weekly*.
Haenggi, M. 2005. Opportunities and challenges in wireless sensor networks. In M. Ilyas and I. Mahgoub, editors, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press.
Hannum, D. 1998, September. Survey of commercially available explosives detection technologies and equipment, Sandia National Laboratories. Available from www.ncjrs.gov/pdffiles1/nij/grants/208861.pdf, last accessed 10 Sep 2007.
Hoke, S., A. Perry, S. Kumar, P. Czipott, B. Whitecotton, T. McManus, & D. Walsh. 2005, May. Using unmanned aerial vehicle-borne magnetic sensors to detect and locate improvised explosive devices and unexploded ordnance. Proceedings of the SPIE, Volume 5778, 963-971.
Kaushik, A., N. Lovell, & B. Celler. 2007, August. Evaluation of PIR detector characteristics for monitoring occupancy patterns for elderly people living alone at home. Proc. 29th Intl. Conf. of Engineering in Medicine and Biology Society, Lyon, France, 3802-3805.
Rouse, G., H. French, H. Sasaki, & T. Kawai. 1995, July. A solid-state vehicle detector for roadway applications. Proc. Vehicle Navigation and Information Systems Conference, 11-16.
Rowe, N. 2005, September. Detecting suspicious behavior from only positional data with distributed sensor networks. 5th International Conference on Multibody Systems, Nonlinear Dynamics and Control, Long Beach, California.
Salatas, V. 2005, September. Object tracking using wireless sensor networks, Masters Thesis, Naval Postgraduate School. Available from stinet.dtic.mil.
Sundram, J., & P. Sim. 2007, December. Using wireless sensor networks in Improvised Explosive Device detection. M. S. thesis, Naval Postgraduate School.
Tran, J., K.-T. Yao, P. Colon, J. Curiel, & M. Anhalt. 2007. Modeling human performance of situation awareness in constructive simulations. *Proc. Interservice/Industry Training, Simulation, and Education Conference*.
U. S. Army. 2005, September. FM 3-34.119/MCIP 3-17.01, Improvised explosive defeat. Available from www.fas.org/irp/doddir/army/fmi3-34-119-excerpt.pdf, last accessed 30 Oct 2007.
U.S. Army. 1992. FM 5-250, *Explosives and Demolition*. Available from www.preterhuman.net/texts/terrorism_and_pyrotechnics/explosives/MISC/Explosives%20and%20Demolitions%20-%20FM%205-250.pdf, last accessed 29 Oct 2007.
U.S. Army, Training and Doctrine Command. 2007. *A Military Guide to Terrorism in the Twenty-First Century*. DCSINT Handbook No. 1.

th

U. S. Department of Homeland Security (DHS). 2002. The support anti-terrorism by fostering effective technologies act of 2002. Available from a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5223.htm, accessed 11 Oct 2007.
Wiegert, R., & J. Oeschger. 2006, September. Portable magnetic gradiometer for real-time localization and classification of unexploded ordnance. *Proc. OCEANS 2006*, 1-6.
XyTrans, Inc. 2006, July. Longer stand-off distance for IED detection. Available from www.xytrans.com/pdf/IED%20Detection%20White%20Paper.pdf, accessed 8 Sep 2007.

Acknowledgements: This work was supported in part by the National Science Foundation under grant 0729696 of the Explosives and Related Threats Exploratory Research Program.

Assessment of Electromagnetic and Passive Diffuse Infrared Sensors in Detection of IED-Related Behavior

Joshua Sundram, Phua Poh Sim, Neil C. Rowe, and Gurminder Singh

U.S. Naval Postgraduate School

ncrowe@nps.edu

June 2008

Overview

- We want to monitor urban public areas for suspicious behavior.
- This is useful for counter-IED operations (besides crime prevention).
- Wireless sensor networks could be a cheaper and more robust alternative to video surveillance.
- Finding suspicious behavior from sensor networks can be automated.
- We experimented with some simple approaches using magnetic and infrared sensors from Crossbow Technologies.
- We ran human subjects through the sensor field while engaged in various activities, some of them suspicious.

Detecting IED emplacement

- Improvised explosive devices (IEDs) are a serious problem in Iraq and now other countries.
- Detection of emplaced (buried or camouflaged) IEDs has been quite unsuccessful in Iraq.
- Tracking down IED organizations (a JIEDDO focus) isn't working well because they are decentralized and adaptive.
- So the best hope is to catch IEDs during emplacement – intrinsically suspicious activity usually involving deception.
- This requires very distributed sensing.

IED components

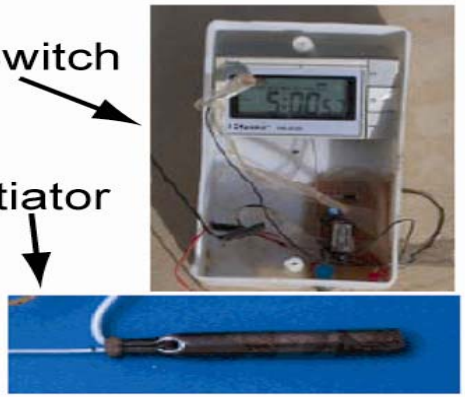
Main Charge

Explosive Filler

Initiating System

Switch

Initiator

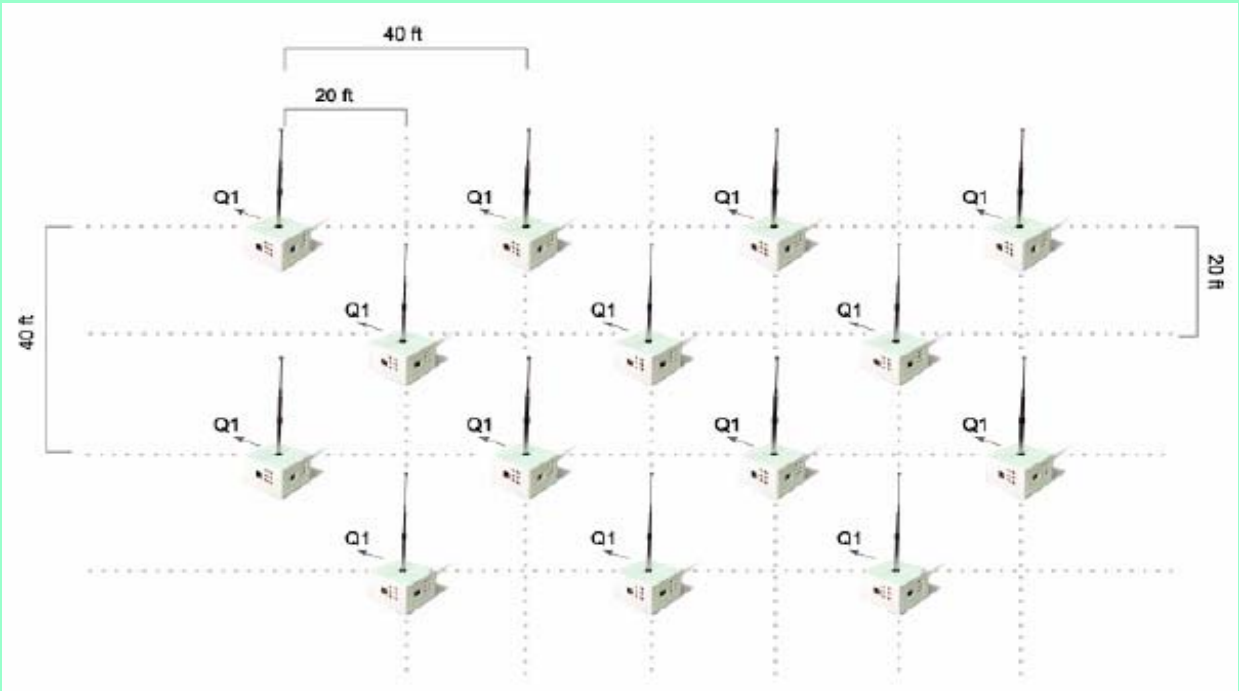


Power Sources

Casing

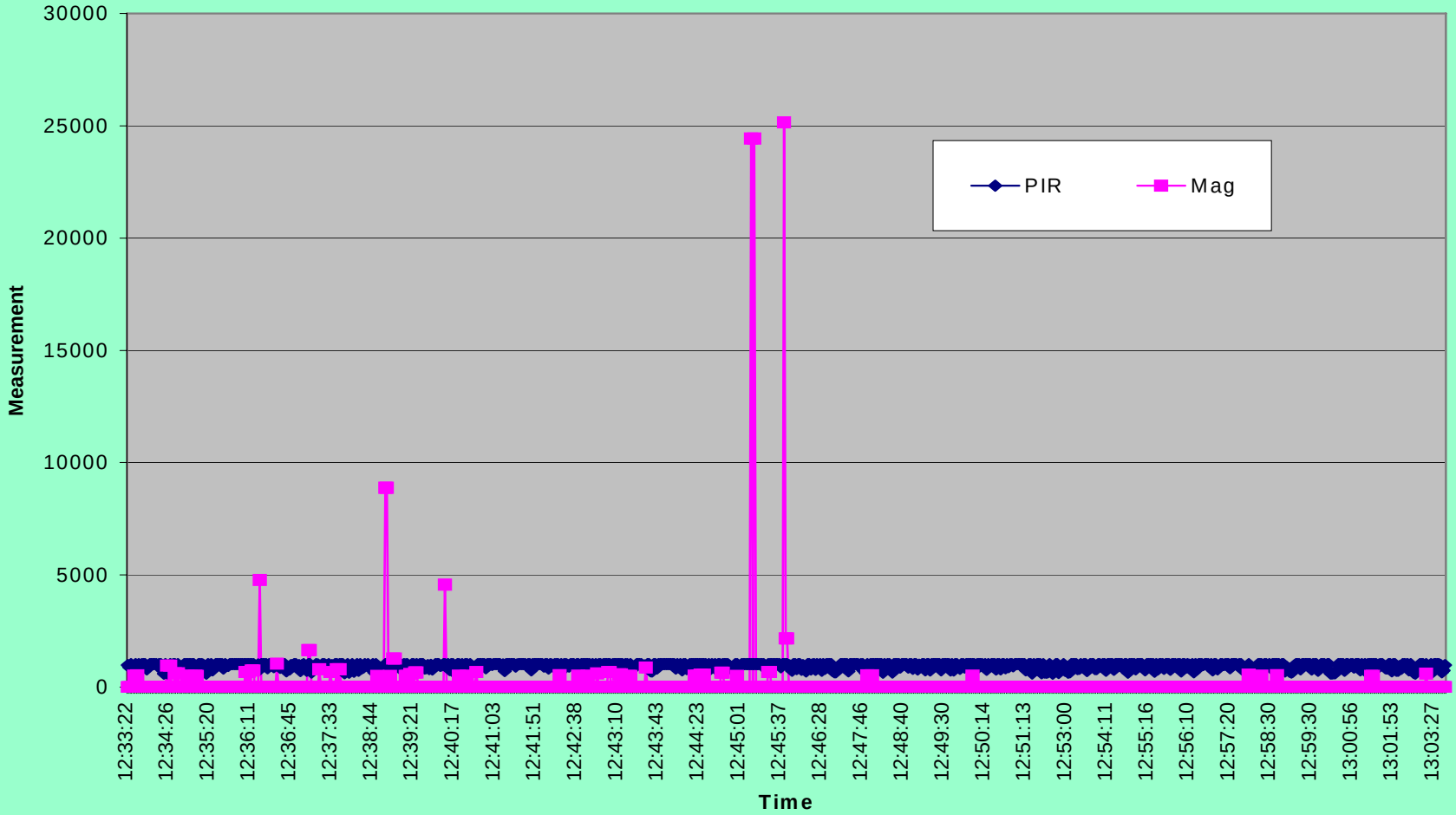
Containers

Crossbow MSP-410 base station, mote, and example dense deployment

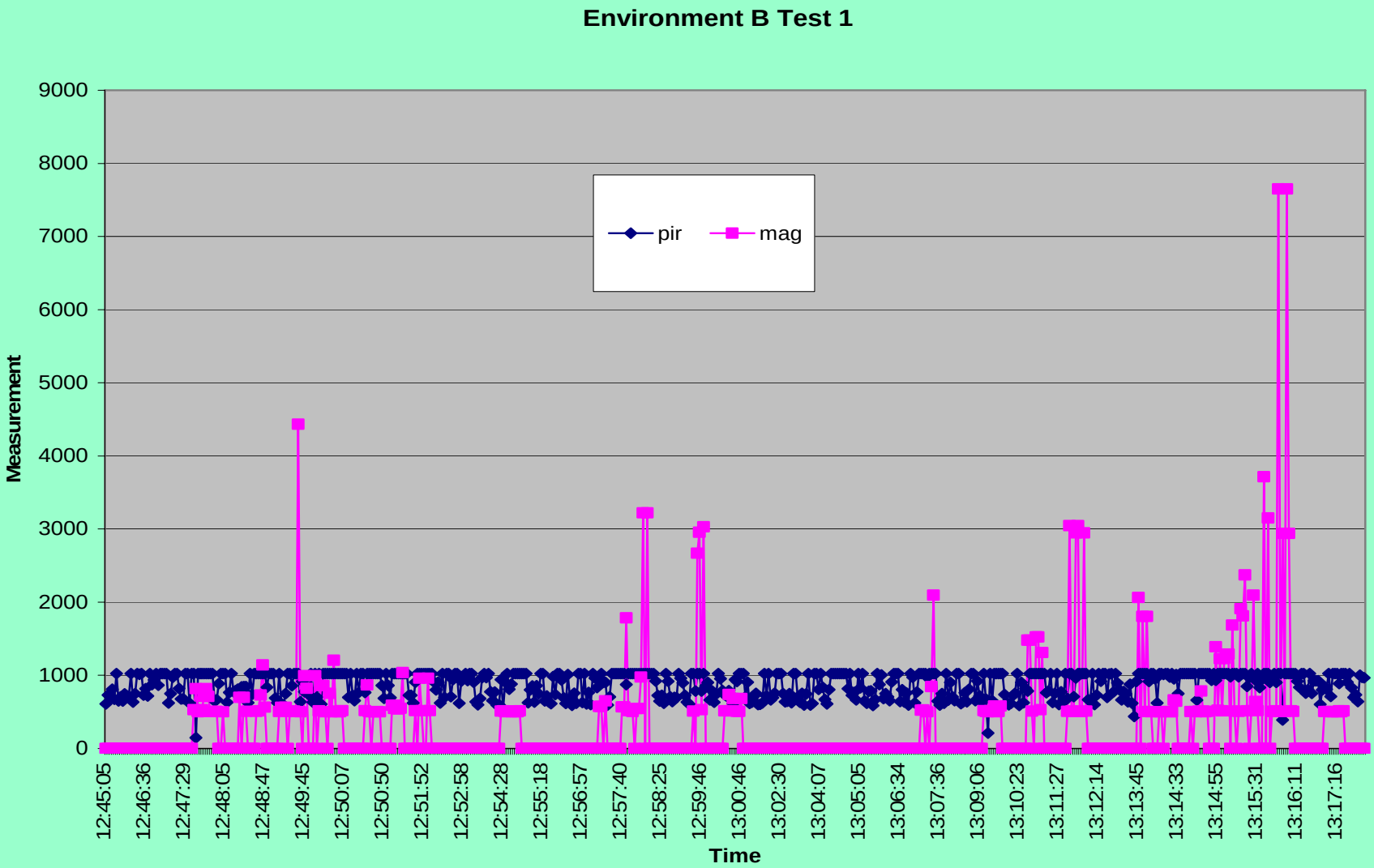


Settings of our first experiments

Signals observed in shopping center



Signals observed along street



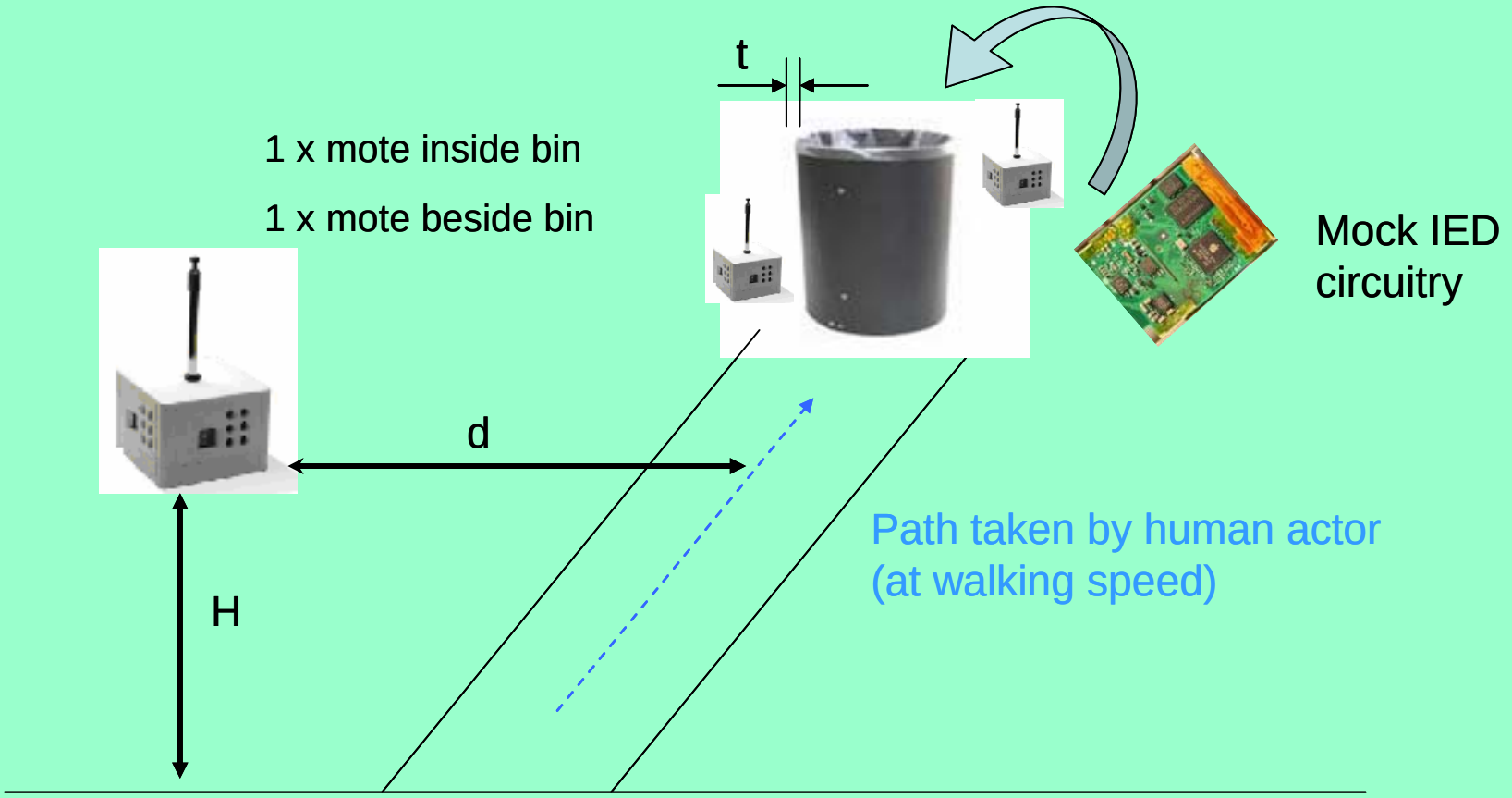
Experiments with magnetic detection of nails

***X* / nails**	**Magnetic readings at H / cm**					
	0		**45**		**80**	
	Distance from mote, d / cm					
	10	**50**	**10**	**50**	**10**	**50**
5	207	144	559	560	488	492
10	215	150	667	596	654	512
20	219	184	882	598	886	534

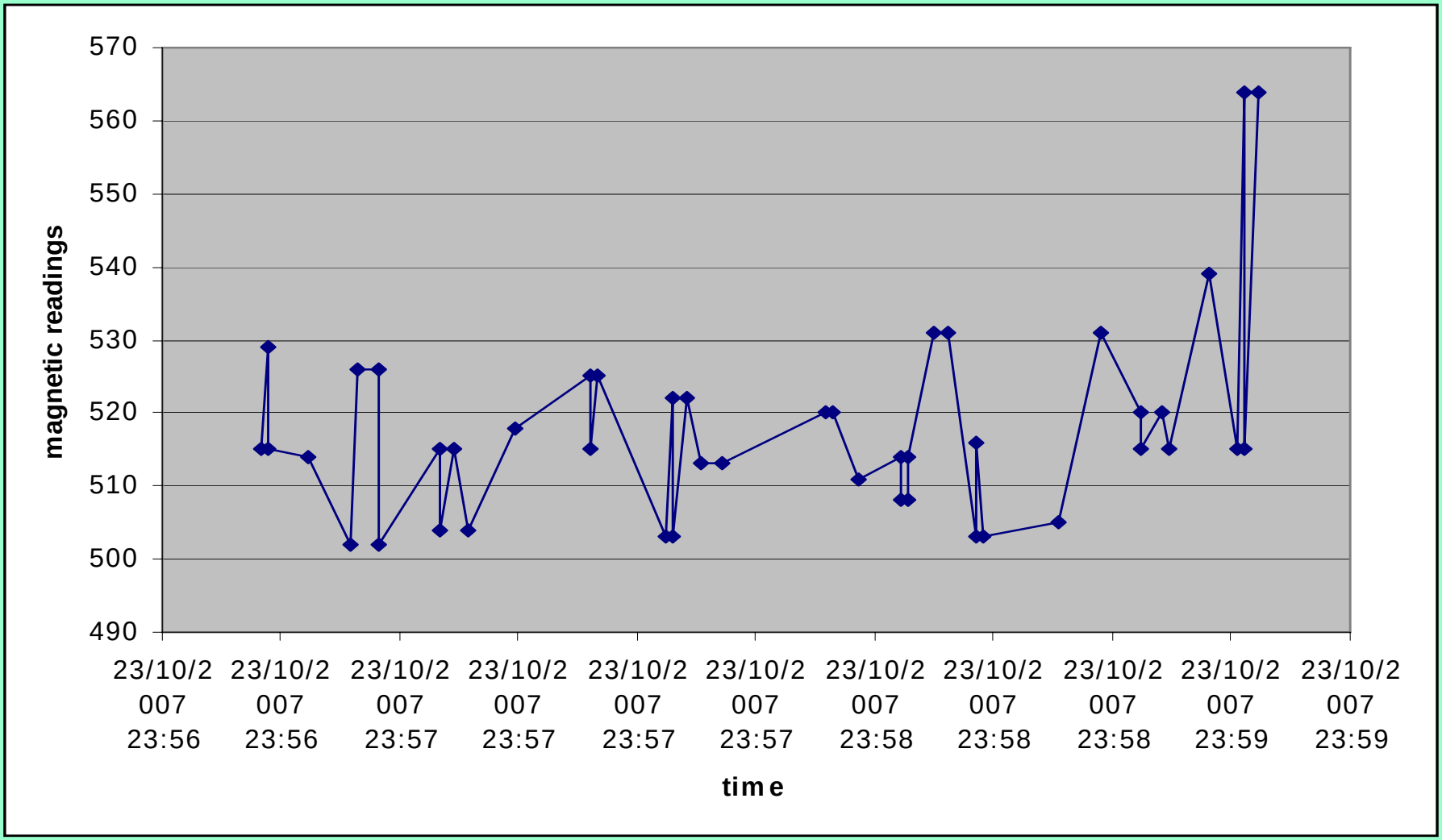
Further nail experiments

H / cm d / cm	Magnetic Readings		
	0	45	80
10	294	589	680
50	221	578	619

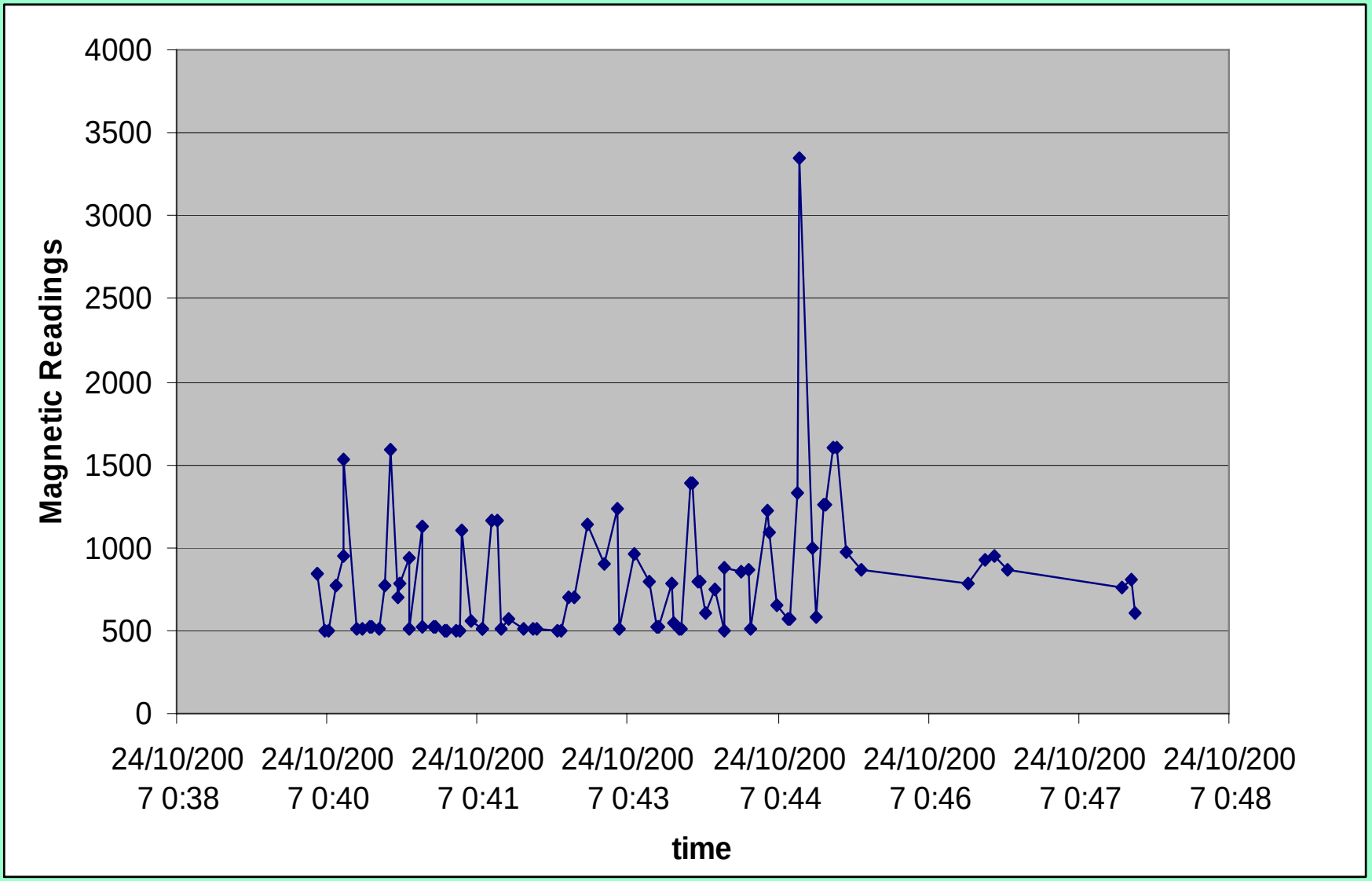
Trash bin experiment



Magnetics: gradual emplacement in bin



Sudden emplacement in bin



Magnetic readings from bin emplacement

H / cm t / cm	Mote 1			Mote 2		
	0	45	90	0	45	90
0.2	0	483	497	509	516	539
0.5	0	285	455	-	-	-
1	0	268	421	-	-	-

Conclusions from these experiments

- Crossbow sensors have trouble characterizing small objects.
- Setting thresholds as average readings is crude – time of day important.
- Diffuse infrared sensors detect humans but this is not useful for IED detection by itself.
- Some close objects were not detected by infrared sensors because the beams were too narrow.
- Infrared sensors were susceptible to air disturbances and temperature variations.
- Magnetic sensors triggered without ferrous materials.
- Magnetic sensors may be more useful in restricted deployments such as in receptacles.
- More motes should be used to reduce false positives.
- Our sensor topology appeared to be a good for areas of limited ingresses and egresses.
- The experiments required high power consumption; design may need to be different when power is more critical.

Subsequent work

- Use of multiple sensors could improve decision making.
- Imaging, seismic, and chemical sensors could improve the selectivity of the thresholds for IEDs.
- Localization in the sensor field can be done with various forms of triangulation.
- Develop explicit clues for suspicious behavior (e.g. nonzero acceleration norms).
- Study concept of contagion of one agent's suspiciousness.
- Behaviors particularly related to IEDs can be sought, e.g. digging for laying a command wire.

New work on detecting suspicious behavior

Suspicious movements for rf20041216_150734fi (Flag: 0)(Scale: 1)(pictures 1 through 440)

initial location: pathID(pic#)(ave of max and ave suspicion)
suspicion(low...high): blue...red

Simpler example: Note halts at trash bin and at car

Suspicious movements for rf20050110_172844fi (Flag: 0)(Scale: 1)(pictures 13 through 336)

initial location: pathID(pic#)(ave of max and ave suspicion)
suspicion(low...high): blue...red

The most useful factor in suspiciousness: Acceleration norm

- Let x(i) be vector position at time i.
- Let N be the number of positions in a track.
- Let d be the time scale.
- Then average acceleration norm can be computed as:

$$a(d) = (1/d(N-2d)) \sum_{i=d+1}^{N-d} \left\| -x(i-d) + 2x(i) - x(i+d) \right\|$$

- The average of a(1), a(2), a(4), a(8), etc. provides a good broad metric of suspiciousness.

Block diagram of proposed system